Mission Assurance Requirements

Section 1. GENERAL

1.1 Description of Overall Requirements

[MAR 101] The Contractor **shall** plan and implement an organized Mission Assurance program to assure the integrity and safety of items critical for mission success that encompasses hardware, software and processes whether designed/built by the Contractor or suppliers, from project initiation through deployment.

[MAR 102] The Contractor **shall** document waivers/deviations and submit them to the Space Network Ground Segment Sustainment (SGSS) Project for approval as described in **SOW CDRL CM-11**. These deviations/waivers will be controlled and maintained by SGSS Configuration Management.

[MAR 103] The Contractor personnel responsible for assurance activities **shall** have direct access to Contractor management, independent of project management, with the functional freedom and authority to interact with other elements of their project.

[MAR 104] The Contractor **shall** ensure that review processes are in place at their level to certify the safety and operational readiness of hardware/software, support equipment, hazardous facilities/operations.

1.2 Surveillance of the Contractor

[MAR 105] The work activities, operations, and documentation performed by the Contractor and suppliers **shall** be subject to evaluation, review, audit, and inspection by designated representatives from NASA, the Government Inspection Agency (GIA), or an Independent Assurance Contractor (IAC).

[MAR 106] The developer **shall** grant access for National Aeronautics and Space Administration (NASA) and NASA assurance representatives to conduct an audit, assessment, or survey upon notice. The developer **shall** supply necessary documents, records, and equipment.

Note: see Federal Acquisition Regulations (FAR) Parts 46.103, 46.104, 46.202-2, 46.4, and 46.5 for government quality assurance requirements at contractor facilities. See FAR Part 52.246 for inspection clauses by contract type.

[MAR 107] The Contractor **shall** provide resources to assist with the assessments/surveys with minimal disruption to work activities.

[MAR 108] The Contractor, upon request, **shall** provide government assurance representatives with documents, records, and equipment required to perform their assurance and safety activities.

[MAR 109] The Contractor **shall** provide the government assurance representative(s) with an acceptable work area within contractor facilities.

1.3 Applicable Documents

[MAR 110] Documents referenced in the Mission Assurance Requirements (MAR) are the effective versions as of the date of Request for Proposal. They form a part of this specification to the extent specified in the requirements.

[MAR 111] In the event of conflict between documents specified in the MAR and other detailed content of the MAR, the MAR **shall** be the superseding document.

1.4 Mission Assurance Implementation Plan

[MAR 112] The Contractor **shall** develop and deliver an SGSS Mission Assurance Implementation Plan (MAIP) (**CDRL MA-02**).

[MAR 113] The Contractor **shall** document the method used to verify compliance for each requirement in the SGSS Requirements Verification Matrix (RVM).

[MAR 114] The Contractor's S&MA function **shall** verify the correctness and completeness of the SGSS Requirements Verification Matrix (RVM).

Section 2. QUALITY MANAGEMENT SYSTEM

2.1 General

[MAR 115] The Contractor and suppliers **shall** have a Quality Management System (QMS) that is compliant with the minimum requirements of ANSI/ISO/ASQC Q9001.

[MAR 116] The Contractor **shall** provide a copy of the Quality Manual to the government (**CDRL MA-03**).

2.1.1 Material Processing

[MAR 117] The Contractor **shall** utilize the SGSS Discrepancy Reporting system for any anomalies that are material-related.

[MAR 118] The material review process **shall** be initiated with the identification and documentation of a material nonconformance.

[MAR 119] Material nonconformance dispositions **shall** include: scrap, rework, return to supplier, repair use-as-is (upon concurrence with the Government Quality Assurance (QA) organization), or request for a waiver.

[MAR 120] All repair procedures proposed for use **shall** have SGSS Project Office approval prior to use.

[MAR 121] For each reported material nonconformance, there **shall** be an investigation and engineering analysis sufficient to determine cause and corrective actions for the nonconformance.

[MAR 122] Written authorization **shall** be documented to disposition the nonconforming product.

[MAR 123] The Contractor **shall** complete all failure analyses on a unit/module, including failure mode, root cause analysis and recommended corrective actions, within 30 days.

2.1.2 Calibration

[MAR 124] The Contractor **shall** have a documented metrology and calibration program.

[MAR 125] The Contractor **shall** comply with ANSI/NCSL Z540.1-1994 Calibration Laboratories and Measuring and Test Equipment – General Requirements.

[MAR 126] The Contractor **shall** limit the use of non-calibrated instruments to applications where substantiated accuracy is not required and for indication-only purposes in non-hazardous, non-critical applications.

2.1.3 Flow-Down of Requirements

[MAR 127] The Contractor **shall** ensure the flow-down of technical and product assurance requirements to suppliers.

[MAR 128] The Contractor Contract Review and Purchasing processes **shall** establish the process for documenting, communicating, and reviewing requirements with suppliers to ensure MAR Requirements are met.

Section 3. SYSTEM SAFETY

3.1 General

[MAR 129] The Contractor **shall** plan and implement a safety program in accordance with NASA Procedural Requirements (NPR) 8715.3 NASA General Safety Program Requirements (a.k.a. NASA Safety Manual) and MIL STD 882.

[MAR 130] The Contractor **shall** initiate the safety program in the concept phase of design and continue throughout all phases of the project as defined by the requirements documents.

[MAR 131] The Contractor **shall** implement a safety program that provides for early identification and control of hazards during design, modifications, construction, fabrication, assembly, test, operation, transportation, and ground activities. The safety program identifies and controls hazards to personnel, facilities, and support equipment, during all stages of development.

[MAR 132] The Contractor **shall** address hazards in the hardware, associated software, ground support equipment, and support facilities to ensure that they meet existing safety standards and/or consensus standards.

[MAR 133] In the event that there are no known applicable standards then special supplemental standards **shall** be developed by the contractor.

[MAR 134] Each System Safety requirement **shall** be addressed by the Contractor.

[MAR 135] In the event a requirement does not apply to a particular program element, the rationale for not complying with that requirement **shall** be presented to the SGSS Project Office prior to approval of the System Safety Program Plan (SSPP).

[MAR 136] The Contractor **shall** plan and implement a system safety program that ensures the following safety requirements:

a) If a system failure may lead to a catastrophic hazard, the system will have three inhibits (dual fault tolerant). A Catastrophic hazard is defined as a hazard that could result in a mishap causing fatal or disabling injury to personnel, and/or loss of one or more major elements of the ground facility or is imparted to the flight vehicle.
b) If a system failure may lead to a critical hazard, the system will have two inhibits (single fault tolerant). A Critical hazard is defined as a condition that may cause severe injury or occupational illness, or major property damage to facilities, systems, or mission critical hardware.
c) Hazards which cannot be controlled by failure tolerance (e.g., structures, pressure vessels, etc.) are called "Design for Minimum Risk" areas of design and have separate, detailed safety requirements that they must meet. Hazard controls related to these areas are extremely critical and warrant careful attention to the details of verification of compliance on the part of the Contractor.

3.2 System Safety Deliverables

3.2.1 System Safety Program Plan

[MAR 137] The Contractor **shall** prepare a System Safety Program Plan (SSPP) **(CDRL MA-04)** in accordance with MIL STD 882.

[MAR 138] The SSPP **shall** describe the system safety implementation process which includes analysis, reduction, and/or elimination of hazards.

[MAR 139] The SSPP **shall** define the required safety documentation, applicable documents, associated schedules for completion, roles and responsibilities on the project, and methodologies for the conduct of any required safety analyses and reviews as defined by NPR 8715.3 NASA Safety Manual.

[MAR 140] The SSPP **shall** be approved by the Goddard Space Flight Center (GSFC) Project Safety Office prior to the contractor performing work on the hardware.

3.2.2 Safety Requirements Compliance Checklist

[MAR 141] The Contractor **shall** develop a Safety Requirements Compliance Checklist (**CDRL MA-05)** that demonstrates that systems and operations are in compliance with safety requirements.

[MAR 142] The Contractor **shall** identify and communicate non-compliant areas to the SGSS Project Office.

3.2.3 Hazard Analyses

3.2.3.1 Preliminary Hazard Analysis

[MAR 143] The Contractor **shall** perform and document a Preliminary Hazard Analysis (PHA) **(CDRL MA-06)** to obtain an initial risk assessment of a concept or system. The purpose of this task is to perform and document a HA to identify safety critical areas, to provide an initial assessment of hazards including software, and to identify recommended hazard controls and follow-on actions.

[MAR 144] The Contractor **shall** submit the necessary design, operations, and analyses data, support meetings, and answered questions to the SGSS Project Office for review.

[MAR 145] The Contractor **shall** evaluate hazards associated with the proposed design or function for hazard severity, hazard probability, and operational constraint based on the best available data, including mishap data from similar systems and other lessons learned.

[MAR 146] The Contractor **shall** include safety provisions and alternatives needed to eliminate hazards or reduce their associated risk to an acceptable level.

3.2.3.2 Operations Hazard Analysis

[MAR 147] The Contractor **shall** perform an Operations Hazard Analysis (OHA) **(CDRL MA-07)** to identify the hazards to personnel and hardware when a facility is being used or an activity is being performed.

[MAR 148] The Contractor **shall** document in the OHA controls and methods of verifications for each hazard listed. The OHA process considers the timing and sequence of tasks with respect to the equipment/hardware/software design, human engineering provisions, assembly, test, and operating procedures, and the facility environments for each specific operation being performed.

3.2.3.3 Software Safety Analysis

[MAR 149] The Contractor **shall** identify hazards caused by software as a part of the nominal hazard analysis process, and their controls will be verified prior to acceptance per NASA-STD- 8719.13B "NASA Software Safety Standard."

[MAR 150] The Contractor **shall** deliver the Software Safety Analysis as part of the Preliminary Hazard Analysis **(CDRL MA-06)**

3.3 Verification Tracking Log

[MAR 151] The Contractor **shall** establish a "closed loop" process for tracking all hazards to acceptable closure through the use of a Verification Tracking Log (VTL) **(CDRL MA-08)**.

[MAR 152] The Contractor **shall** close individual VTL items with appropriate documentation verifying the stated hazard control has been implemented.

[MAR 153] The Contractor **shall** complete individual closures prior to first operational use/restraint.

3.4 Safety Non-Compliance/Waiver Requests

[MAR 154] When a specific safety requirement cannot be met the Contractor **shall** submit an associated safety noncompliance/waiver request which identifies the hazard and shows rationale for approval of the waiver.

[MAR 155] The Contractor **shall** deliver the Safety Noncompliance/Waiver Requests in accordance with **(CDRL MA-09).**

3.5 Support for Safety Working Group Meetings

[MAR 156] The Contractor **shall** provide technical support at Project Safety Working Group meetings (SWG), Technical Interface Meetings (TIM), and technical reviews. The SWG will meet as necessary to review procedures and analyses that contain or examine safety critical functions or as convened by the Project Safety Manager (PSM) to discuss any situations that may arise with respect to overall project safety.

3.6 Mishap Reporting

[MAR 157] The Contractor **shall** report mishaps, incidents, hazards, and close calls in accordance NPR 8621.1, NASA Procedural Requirements For Mishap And Close Call Reporting.

3.7 Pre-Mishap Contingency Plan Inputs

[MAR 158] The contractor **shall** develop a Pre-Mishap Contingency Plan (**CDRL MA-10)** inputs to the SGSS Project Office prior to initiating any project operations with potential for personnel injury or hardware damage.

[MAR 159] The Contractor **shall** maintain a notification list and provide a copy to support the Project Pre-Mishap Contingency Plan. The Pre-Mishap plan inputs ensure that contingency plans are in place to properly secure a mishap site, impound evidence, and provide necessary notification within the program and to designated Agency notification contacts. The security of personnel and physical resources under the control of the project are also considered in the plan.

[MAR 160] The Pre-Mishap Plan Inputs **shall** describe the procedures to comply with NPR 8621.1, NASA Procedural Requirements For Mishap And Close Call Reporting, Investigating, and Recordkeeping.

Section 4. PROBABILITY RISK ANALYSIS AND RELIABILITY, MAINTAINABILITY AND AVAILABILITY

4.1 Probabilistic Risk Assessment and Reliability, Maintainability and Availability (RMA) Program Plan

[MAR 161] The Contractor **shall** prepare, submit and implement an integrated (hardware and software) Probabilistic Risk Assessment (PRA) and Reliability, Maintainability, and Availability (RMA) Program Plan (**CDRL MA-11**) using both qualitative and quantitative techniques to support decisions regarding mission success and safety throughout all life cycle phases as appropriate.

[MAR 162] Equipment vendors, subcontractors and/or suppliers **shall** provide inputs to the development and implementation of the GS RMA Plan, through and as directed by the GS Project.

[MAR 163] The Contractor **shall** present the implementation of the PRA and the RMA Program Plan and related activities at milestone reviews beginning with the System Requirements Review.

[MAR 164] The Contractor **shall** specify in the RMA Program Plan how to define, measure, control, and report on RMA in all lifecycle phases as appropriate.

[MAR 165] Starting in the conceptual design stage the Contractor **shall** clearly define and evaluate levels of performance based upon SRD reliability, maintainability and availability requirements.

[MAR 166] The Contractor **shall** allocate RMA requirements to the architecture component level as appropriate. RMA requirements will be used to establish baseline requirements against which the design alternatives are evaluated. Requirements consistent with the allocations will be imposed on any subcontractors, suppliers and/or COTS vendors whenever appropriate.

[MAR 167] The Contractor **shall** continue RMA activities throughout the Period of Performance in accordance with the RMA Plan (**CDRL MA-11**), replacing calculated data analysis with analysis of the actual reliability and maintainability statistics of the GS, as well as updating analyses to cover any changes in configuration, hardware, or software.

[MAR 168] The Contractor **shall** track and report the operational availability metrics as cumulative downtime metrics on a weekly basis starting with "Shadow Operations" (TBR) of the transition.

[MAR 169] The Contractor **shall** ensure that the SNGN/SGSS has no silent failures. A silent failure is any equipment failure that would result in either a loss of service or a loss of protection without an audible alarm and/or remote signaling to initiate corrective action.

[MAR 170] The Contractor **shall** implement corrective actions whenever reliability, maintainability, and availability related requirements are not satisfied.

[MAR 171] The Contractor **shall** prepare and submit Reliability, Maintainability and Availability Prediction and Model Reports (**CDRL MA-12**).

[MAR 172] The Contractor **shall** perform maintainability evaluation and demonstration tests to verify that all preventive and corrective maintenance activities, such as system and data level backups, can be successfully executed.

[MAR 173] The Contractor **shall** prepare and submit Maintainability Demonstration Reports (**CDRL MA-13**).

[MAR 174] The Contractor **shall** ensure and document that line replaceable units critical to the performance of the SGSS, that suffer a failure after being repaired twice, are not returned to service.

[MAR 175] The Contractor **shall** provide a sparing plan in accordance with **CDRL MO-05** that takes into account the failure rates of line replaceable units as well as logistics-related times such as replenishment times and processing times.

4.2 Maintainability

[MAR 176] The Contractor **shall** based on the definition of acceptable levels of performance, define the following minimum acceptable maintainability parameters for all hardware and software:

1. Diagnostic time to detect and fault isolate to the defective components/sub-systems/applications.

2. Time required to codify and integrate updates to the defective components/sub-systems/applications.
3. Time required to complete checkout and restore operational status.

[MAR 177] The Contractor **shall** establish and implement specific design criteria needed to mitigate unacceptable levels of performance.

[MAR 178] The Contractor **shall** make accessible design criteria for Government review at anytime and present at all formal design reviews in conjunction with the RMA Program Plan updates (**CDRL MA-11**).

[MAR 179] The Contractor **shall** assure that software, equipment, and components obtained from COTS and GOTS providers meet allocated reliability, maintainability and availability requirements.

[MAR 180] The Contractor **shall** verify and assure that equipment and components obtained from subcontractors, suppliers, and COTS/GOTS providers, including GFPs, meet allocated requirements. If not, the Contractor **shall** report such discrepancies to the SGSS PM for review per **SOW CDRL PM-17**.

[MAR 181] The Contractor **shall** develop and implement specific design criteria to facilitate maintenance or repair activities.

[MAR 182] The Contractor **shall** use data obtained from similar system installations in establishing maintainability design criteria that meet the specifications.

[MAR 183] The Contractor **shall** include design for modularity, accurate fault diagnostics, standardization, and commonality in the design criteria.

4.3 Probabilistic Risk Assessment (PRA)

[MAR 184] The Contractor **shall** perform a PRA encompassing the mission critical hardware and software modules. **(CDRL MA-15)**.

[MAR 185] The scope of the PRA **shall** be commensurate with the risk classification per Table 1 of NPR 8705.5.

[MAR 186] The PRA **shall** address equipment failures and degraded modes of operation.

4.4 Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL)

[MAR 187] The Contractor **shall** perform a Failure Modes and Effects Analysis (FMEA) for all mission critical hardware and software **(CDRL MA-16)** and prepare and maintain a Critical Items List (CIL) **(CDRL MA-16)**.

[MAR 188] Equipment vendors, subcontractors and/or suppliers, including GFP vendors **shall** provide relevant inputs to the development and implementation of the SGSS FMEA, through and as directed by the SGSS Project.

[MAR 189] The Contractor **shall** assign each failure mode a severity category in accordance with the FMEA Severity Categories Table based on the most severe effect caused by the failure:

FMEA Severity Categories Table

Category	FMEA Severity Categories	Description
1	Catastrophic	Failure modes that could result in serious injury, loss of life, or loss of satellite, or launch vehicle.
1R	Catastrophic	Failure modes of identical or equivalent redundant hardware items that, if

		all failed, could result in Category 1 effects.
1S	Catastrophic	Failure in a safety or hazard monitoring system that could cause the system to fail to detect a hazardous condition or fail to operate during such condition and lead to Severity Category 1 consequences.
2	Critical	Failure modes that could result in the loss of one or more mission objectives as defined by the SGSS PM.
2R	Critical	Failure modes of identical or equivalent redundant hardware items that could result in Category 2 effects if all failed.
3	Significant	Failure modes that could cause degradation to mission objectives.
4	Minor	Failure modes that could result in insignificant or no loss to mission objectives.

[MAR 190] The Contractor **shall** itemize on the Critical Items List (CIL) and **shall** analyze at a greater depth failure modes resulting in FMEA Severity Categories 1, 1R, 1S or 2 of the FMEA Severity Categories Table.

[MAR 191] The Contractor **shall** provide in the FMEA report the Rationale for including items on the CIL.

[MAR 192] The Contractor **shall** analyze single point failure modes to determine the root cause, corresponding mitigation actions, and retention rationale.

[MAR 193] The Contractor **shall** address in the FMEA hardware and software that is designed, built, or provided by their organization or subcontractors, from project initiation through mission operations.

[MAR 194] When redundancies are required, the Contractor **shall** analyze in the FMEA such redundancies to ensure that redundant paths are isolated or protected such that any single failure that causes the loss of a functional path will not affect the other functional path(s) or the capability to switch operation to that redundant path.

[MAR 195] The Contractor **shall** use the results of the FMEA to evaluate the design relative to requirements.

[MAR 196] The Contractor **shall** ensure that discrepancies identified in the FMEA are evaluated by SGSS management and design groups for assessment of the need for corrective actions.

[MAR 197] The Contractor **shall** document and present how the FMEA was used to perform design tradeoffs and how the FMEA results were taken into consideration making design or risk management decisions.

[MAR 198] The contractor **shall** use the FMEA to assist in the development of planned maintenance activities required to operate the system.

[MAR 199] Results of the FMEA **shall** be presented at design reviews starting with the Preliminary Design Review.

4.5 Fault Tree Analysis

[MAR 200] The Contractor **shall** perform qualitative fault tree analyses (FTAs) to address mission failures and degraded modes of operation.

[MAR 201] The Contractor **shall** perform quantitative fault tree analyses to address undesirable fault propagation scenarios as part of the PRA **(CDRL MA-17).**

[MAR 202] The Contractor **shall** address in the FTA safety critical software as defined in NASA-STD-8719.13 that is identified as part of the FMEA process.

4.6 Parts Stress Analysis

[MAR 203] The Contractor **shall** perform parts stress and derating analyses for electrical, electronic, and electromechanical (EEE) parts in accordance with GSFC INST-EEE-002 **(CDRL MA-18).**

[MAR 204] The Contractor **shall** take corrective action when the Parts Stress Analysis identifies stressed electrical, electronic, and electromechanical parts.

4.7 Worst Case Analysis

[MAR 205] The Contractor **shall** perform worst case analyses for circuits **(CDRL MA-19).**

4.8 Availability Assessments and Predictions

[MAR 206] The Contractor **shall** substantiate Availability with:

- Measures of Mean Time Between Failure (MTBF) and Mean Time To Repair (MTTR) for all hardware and software CIs.
- Reliability Block Diagrams and Predictions Report **(CDRL MA-12)** and analyses addressing redundancies including hardware and software components.
- Measures of Max Time to Restore Service (MaxTTRS) for all hardware and software CIs

[MAR 207] The Contractor **shall** perform and report comparative numerical RMA predictions **(CDRL MA-12)** to validate that the design meets the requirements of the specification and to assist with:

a) Evaluation of alternative design concepts, redundancy, and - failover approaches.
b) Identification of the elements of the design, which lowest reliability or highest maintenance cost.
c) Identification of potential mission-limiting elements and components that will require special attention in part selection, testing, environmental isolation, and/or special operations.
d) Evaluation of the impact of proposed engineering change and waiver requests.

[MAR 208] The Contractor **shall** use the following sources of failure rates for the reliability predictions:

a) Performance of similar items (with approval of SGSS program management
b) Test data at the 95% confidence level (with approval of SGSS program management)
c) MIL-HDBK-217F - Reliability Prediction of Electronic Equipment with updated failure rates (e.g., "Handbook of 217 Plus", "MIL-HDBK-472") from the Reliability Information Analysis Center, or equivalent.
d) Telcordia SR-322 v2, after approval by SGSS program management.

[MAR 209] The Contractor **shall** submit assessments and updates to the SGSS Project Office in accordance with the RMA Predictions Report **(CDRL MA-12).**

[MAR 210] The results of reliability/availability assessments and predictions, particularly those impacting design or risk management decisions, **shall** be reported at Risk Management meetings and PDR and CDR.

4.9 Trend Analysis

[MAR 211] The Contractor **shall** prepare and maintain a list of subsystem and components to be assessed, parameters to be monitored, and trend analysis reports as defined in the approved PRA and Reliability Program Plan.

[MAR 212] The Contractor **shall** begin the monitoring, collection, and analysis at component acceptance testing and continue through the system integration and test phases until the end of the project **(CDRL MA-20).**

[MAR 213] The Contractor **shall** document and report the analysis of test information, trend data, and failure investigations with respect to reliability and maintainability and report the results as defined in the approved PRA and Reliability Program Plan **(CDRL MA-20).**

4.10 Limited Life Items

[MAR 214] The Contractor **shall** prepare and implement a plan to identify and manage limited life items **(CDRL MA-21).**

[MAR 215] Identified limited-life items **shall** be controlled from the date of manufacture through operational use, including storage.

4.11 Life Cycle Cost

[MAR 216] The Contractor **shall** provide estimates of the number of personnel and the amount of maintenance activity that are required to operate and maintain the SNGN/SGSS at the stated reliability and quality levels.

[MAR 217] Life cycle cost models and predictions **shall** be documented, reported and presented in the PDR and CDR (**CDRL MA-22**)

[MAR 218] The Contractor **shall** establish a mechanism that ensures the delivery of critical and long lead-time items before they are required.

Section 5. SOFTWARE ASSURANCE (FLIGHT AND GROUND SEGMENTS)

5.1 Applicable Requirements

[MAR 219] The Contractor **shall** comply with the following for software, databases, and firmware, hereafter collectively referred to as software:

- NPR 7150.2 NASA Software Engineering Requirements
- NASA-STD-8719.13 NASA Software Safety Standard
- NASA-STD-8739.8 NASA Standard for Software Assurance

5.2 Software Quality Assurance

[MAR 220] The Contractor **shall** prepare and implement a software quality assurance plan for software, including government off-the-shelf software (GOTS), modified off-the-shelf software (MOTS), and commercial off-the-shelf software (COTS) **(CDRL MA-23).**

[MAR 221] The Contractor **shall** identify the organizational entity responsible for directing and managing the software quality assurance program.

5.3 Software Reliability

[MAR 222] The contractor **shall** develop and a software reliability program that includes a process for measuring and analyzing defects in the software products during development activities in order to identify and address possible problem areas within the software. (**CDRL MA-11**)

[MAR 223] The contractor **shall** tailor the software reliability program to the appropriate level based upon criticality of the software to the mission, software safety criticality, software complexity, cost, consequence of failure, and other parameters.

[MAR 224] The Contractor **shall** prepare and implement a Software Reliability program that is compliant with IEEE-Std- 1633 *IEEE Recommended Practice on Software Reliability* or an alternate Software reliability program that is approved by the SGSS Project Office.

[MAR 225] The Contractor **shall** assure that fault tolerance and redundancy have been specified and implemented correctly, and verified by testing.

[MAR 226] The Contractor **shall** perform analysis and measurements on all software modules to find specific software modules which may have reliability problems.

[MAR 227] The Contractor **shall** document, monitor, analyze and track software metrics during each stage of development and across development and operational phases. Examples include fault counts by severity levels, time between discovery and fault removal, and number of faults found in a time period per lines of code.

[MAR 228] The Contractor **shall** include in the software metrics the collection and classification of software defects.

[MAR 229] The Contractor **shall** define and make readily available the software metrics required to implement IEEE-Std-1633 to the SGSS Project Office upon request.

[MAR 230] The Contractor **shall** utilize the unified CM and Anomaly Reporting and Tracking system to provide software problem reporting and corrective action reporting and tracking that addresses reporting, analyzing and correcting of software non-conformances and software test failures throughout the development lifecycle starting at PDR.

[MAR 231] The Contractor **shall** provide for a corrective action process that tracks every software nonconformance to its final disposition."

[MAR 232] The Contractor **shall** report all software reliability activities at SGSS project milestone reviews (**CDRL MA-12**).

[MAR 233] The Contractor **shall** submit the selected Reliability Growth Model for approval by the SGSS Project Office no later than Preliminary Design Review.

[MAR 234] The Contractor **shall** perform and report trend analysis on the software defects (**CDRL MA-20**) and make the analysis results available for lessons learned and root cause analysis.

Section 6. WORKMANSHIP STANDARDS

6.1 General

[MAR 235] The Contractor **shall** implement a Workmanship Program for SGSS hardware to assure that workmanship, electronic packaging technologies, and process activities are selected and applied to meet mission objectives for quality and reliability.

[MAR 236] The Contractor **shall** use the IPC-J-STD-001D (Class 3 Requirements) workmanship standard. However, it is recognized that contractors may wish to use similar but not identical workmanship standards, procedures and training.

[MAR 237] Any such alternatives **shall** be accompanied by a comparison to the standards and a discussion of significant differences and rationale for use of the alternative.

6.2 Training and Certification

[MAR 238] The Contractor personnel working on SGSS hardware **shall** maintain certification of successful workmanship training appropriate to their involvement.

[MAR 239] The workmanship certification **shall** include successful completion of formal training and demonstrated performance in the appropriate discipline as defined in the Contractor's applicable requirements.

[MAR 240] The Contractor **shall** document the procedures and processes of their training program.

6.3 Documentation

[MAR 241] The Contractor **shall** document the procedures and processes that will be used to implement the referenced workmanship, design, and ESD control standards.

6.4 Handling

[MAR 242] The Contractor **shall** institute handling (including storage) procedures to prevent part and material degradation for mission essential items in accordance with NPR 6000.1, "Requirements for Packaging, Handling, and Transportation for Aeronautical, and Space Systems, Equipment, and Associated Components."

[MAR 243] Mission essential items are defined in NPR 6000.1 as items that would adversely affect the project in the event of loss, damage, or delay in shipment.

[MAR 244] The following criteria **shall** be used for establishing handling and storage procedures for parts and materials:

- Control of environment, such as temperature, humidity and contamination.
- Measures and facilities to segregate and protect parts and materials routed to different locations such as, to the materials review crib, or to a laboratory for inspection, or returned to the manufacturer from unaccepted shipments.
- Facilities, if needed, for interim storage of parts and materials.
- Provisions for protective cushioning, as required, on storage area shelves, and in storage and transportation containers.
- Protective features of transportation equipment design to prevent packages from being dropped or dislodged in transit.
- Protective bench surfaces on which parts and materials are handled during operations such as test, assembly, inspection, and organizing kits.
- Provisions for protection of parts susceptible to damage by electrostatic discharge.

6.5 Preservation and Packaging

[MAR 245] Parts that are subject to degradation by electrostatic discharge **shall** be packaged in accordance with the approved Electrostatic Discharge (ESD) procedures.

Section 7. COMPONENT, MODULE, AND UNIT CONTROL

7.1 General

[MAR 246] The Contractor **shall** verify that Units and Modules are manufactured, processed, screened, and qualified, as a minimum, to good commercial practice in accordance with UL-60950-1 Information Technology Equipment - Safety Part 1 - General Requirements.

[MAR 247] For appropriate hardware systems, the Contractor **shall** develop and submit to the SGSS Project Office a copy of the electrical, electronic, electro-mechanical (EEE) Parts List **(CDRL MA-24).**

[MAR 248] The Contractor **shall** provide appropriate detailed drawings and component detail for units and assemblies.

[MAR 249] Any modification to COTS products/components **shall** be subject to SGSS project concurrence.

7.2 Custom or Advanced Technology Devices

[MAR 250] All custom technology devices such as custom microcircuits, hybrid microcircuits, Multi-Chip Module (MCM's), Application Specific Integrated Circuits (ASIC's), etc., **shall** be subjected to a review by the SGSS Project Office.

[MAR 251] The Contractor **shall** fully identify in procurement documentation or specification custom devices being procured and include physical, mechanical, electrical, and environmental test requirements and quality assurance provisions necessary to control manufacture and acceptance.

7.3 Equipment Lists

[MAR 252] The Contractor **shall** create and maintain an Equipment (Units and Modules) Identification List (EIL) **(CDRL MA-25).**

[MAR 253] The Contractor **shall** identify equipment used in hardware in the EIL. The EIL is prepared from design team inputs or supplier inputs, and updated to record the delivered and installed hardware.

[MAR 254] The Contractor **shall** include at a minimum the following information in the EIL: number, name or description, manufacturer, manufacturer's generic number, drawing number, specifications, comments as necessary to indicate problems, long lead times, additional testing imposed, and application unique notes.

7.4 Lead-free and Tin Whisker Control

[MAR 255] The Contractor **shall** meet the requirements of GEIA-STD-0005-1 and GEIA-STD-0005-2 for solders and surface finishes that are less than 3% lead by weight.

- GEIA –STD-0005-1: Performance Standard for Aerospace and High Performance Electronics Systems Containing Lead-free Solder
- GEIA-STD-0005-2: Standard for Mitigating the Effects of Tin Whiskers in Aerospace and High Performance Electronic Systems

[MAR 256] The Contractor **shall** prepare, implement and submit a lead-free control plan **(CDRL MA-26)** according to GEIA-STD-0005-2, Control Level 2C.

Section 8. TESTING OF SPARE HARDWARE

8.1 General

[MAR 257] As a minimum, verification testing of spares for hardware **shall** be included in the Ground Segment Performance Verification Plan.

[MAR 258] The same quality and reliability standards and processes used to manufacture original hardware **shall** be used in spares manufacturing and repair processes.

8.2 Extent of Testing

[MAR 259] The extent and type of testing of spares for hardware **shall** be determined as part of the Ground Segment Performance Verification Plan.

8.3 Rework of Spares

[MAR 260] The Contractor **shall** conduct appropriate regression or re-verification testing if a hardware item is removed for reasons of failure and is then repaired and re-designated as a spare.

Section 9. TEST FACILITY READINESS

9.1 General

[MAR 261] The Contractor **shall** verify the readiness of each test, test equipment, and the test facility and document it as part of the Test Readiness Review.

[MAR 262] Equipment used for tests **shall** be in current calibration and so noted by tags and stickers.

Section 10. ELECTROSTIC DISCHARGE (ESD) CONTROL

10.1 General

[MAR 263] The Contractor **shall** document and implement an ESD Control Program in accordance with ANSI/ESD S20.20

[MAR 264] The Electrostatic Discharge Control (ESD) plan **shall** be submitted and approved (**CDRL MA-27**).

Section 11. Government-Industry Data Exchange Program (GIDEP) ALERTS AND PROBLEM ADVISORIES

11.1 General

[MAR 265] The Contractor **shall** participate in GIDEP to evaluate and disposition GIDEP ALERTS, GIDEP SAFE-ALERTS, GIDEP Problem Advisories, GIDEP Agency Action Notices, as well as NASA Advisories to determine if they affect the products produced for SGSS. The following applicable documents apply: S0300-BT-PRO-010, GIDEP Operations Manual, and S0300-BU-GYD- 010 Government Industry Data Exchange Program Requirements Guide.

[MAR 266] For GIDEP ALERTS, GIDEP SAFE-ALERTS, GIDEP Problem Advisories, GIDEP Agency Action Notices, and NASA Advisories that are determined to affect the program, the Contractor **shall** report said Alerts to the SGSS Project Office, as well as respond to SGSS Project Office GIDEP and NASA Advisory notices.

[MAR 267] All GIDEP mitigation approaches shall have prior SGSS Project Office approval.

APPENDIX A Applicable Documents

AFSPCMAN 91-710, Range Safety User Requirements

ANSI/ESD S20.20 Electrostatic Discharge Control Program Standard

ANSI/ISO/ASQC Q9001 - American National Standard Quality Management Systems-Requirements

ANSI/NCSL Z540.1-1994 Calibration Laboratories and Measuring and Test Equipment – General Requirements

GEIA-STD-0005-1: Performance Standard for Aerospace and High Performance Electronics Systems Containing Lead-free Solder

GEIA-STD-0005-2: Standard for Mitigating the Effects of Tin Whiskers in Aerospace and High Performance Electronic Systems

GIDEP Operations Manual (SO300- BT-PRO-010)

GIDEP Requirements Guide (S0300-BU-GYD-010)

GSFC EEE-INST-002 <http://nepp.nasa.gov/DocUploads/FFB52B88-36AE-4378-A05B2C084B5EE2CC/EEE-INST-002_add1.pdf>

GSFC Flight Assurance Procedure, FAP P-322-208, Performing a Failure Mode and Effects Analysis (to be replaced by GSFC-STD-8000)

GSFC Form 4-37, "Problem Impact Statement Parts, Materials and Safety"

GSFC INST-EEE-002 Instructions for EEE Parts Selection, Screening, and Qualification

IEEE Standard 730-2002, Software Quality Assurance Plans

IEEE-Std- 1633 IEEE Recommended Practice on Software Reliability

IPC-J-STD-001D Requirements for Soldered Electrical and Electronic Assemblies (Class 3 requirements)

ISO 10013 Quality Manual Development Guide

MIL-HDBK-217F - Reliability Prediction of Electronic Equipment

MIL-STD-882 System Safety Program Requirements/Standard Practice for System Safety

NASA Fault Tree Handbook with Aerospace Applications (http://www.hq.nasa.gov/office/codeq/doctree/fthb.pdf)

NASA-STD-8719.13B NASA Software Safety Standard.

NASA-STD-8729.1, Planning, Developing and Managing an Effective Reliability and Maintainability (R&M) Program

NASA-STD-8739.8, NASA Standard for Software Assurance

NPD 8720.1, NASA Reliability and Maintainability (R&M) Program Policy

NPD 8730.2 NASA Parts Policy

NPR 6000.1, Requirements for Packaging, Handling, and Transportation for Aeronautical, and Space Systems, Equipment, and Associated Components

NPR 7150.2 NASA Software Engineering Requirements

NPR 8621.1, NASA Procedural Requirements for Mishap Reporting, Investigating, and Recordkeeping

NPR 8705.4 Risk Classification for NASA Payload

NPR 8705.5 PRA Procedures for NASA Programs and Projects

NPR 8715.3 NASA General Safety Program Requirements

NPR 8715.7 Expendable Launch Vehicle Payload Safety Program

NPR-6000.1, Requirements for Packaging, Handling, and Transportation for Aeronautical, and Space Systems, Equipment, and Associated Components

PRA Procedures Guide for NASA Managers and Practitioners (http://www.hq.nasa.gov/office/codeq/doctree/praguide.pdf)

SAE ARP5580 Recommended Failure Modes and Effects Analysis (FMEA) Practices for NON-Automobile Applications

SAE AS9100 Quality Systems - Aerospace - Model for Quality Assurance in Design, Development, Production, Installation and Servicing

Telcordia SR-322 v2

UL-60950-1 Information Technology Equipment,- Safety Part 1 - General Requirements

APPENDIX B Acronyms

ANSI American National Standards Institute
COTS Commercial Off The Shelf
CIL Critical Items List
EEE Electrical, Electronic, and Electromechanical
ESD Electro-Static Discharge
FAR Federal Acquisition Regulations
FAR Final Acceptance Review
FTA Fault Tree Analysis
FMEA Failure Modes and Effects Analysis
GEIA Global Emissions Inventory Activity
GIA Government Inspection Agency
GIDEP Government-Industry Data Exchange Program
GOTS Government Off The Shelf
GSFC Goddard Space Flight Center
IAC Independent Assurance Contractor
MAIP Mission Assurance Implementation Plan
MAR Mission Assurance Requirements
MCM Multi-Chip Module
MOTS Modified Off The Shelf
NASA National Aeronautic and Space Administration
NCSI National Centre for Science Information
NPR NASA Procedural Requirements
OHA Operations Hazard Analysis
PM Program Management
PRA Probabilistic Risk Assessment
QA Quality Assurance
QMS Quality Management System
RMA Reliability Maintainability Availability
SGSS Space Network Ground Segment Sustainment
SNGS Space Network/Ground Segment
SSPP System Safety Program Plan
SWG Safety Working Group
TIM Technical Interface Meeting
VTL Verification Tracking Log